ABSTRACT

PSEUDO-RANDOM NUMBER GENERATOR

The present invention provides a method and an apparatus for generating pseudo-random numbers with very long periods and very low predictability. A seed random sequence is extended into a much longer sequence by successive iterations of matrix operations. Matrices of candidate output values are multiplied by non-constant transition matrices and summed with non-constant offset matrices; the result is then processed through one or more modulus operations, including non-constant modulus operators, to generate the actual output values. The invention also includes the possibility of introducing non-invertible matrices into the operations. The invention creates final results that are equidistributed over large samples. Secondary pseudo-random and other processes determine the non-constant transition matrices, offset matrices, and modulus operators.